

## **Exhibit A**

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF VIRGINIA

ANAS ELHADY, et al.	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Case No. 1:16-cv-375
	)	
CHARLES H. KABLE, et al.	)	
	)	
Defendants.	)	
	)	

**SUPPLEMENTAL RESPONSE**

In accordance with the Court's January 4, 2019 Order, and subject to all previous objections, the TSC provides the following supplemental response to Interrogatory 30 directed to the Terrorist Screening Center (TSC) and related questions at the March 1, 2018 deposition of Timothy P. Groh:

***Interrogatory 30: Identify all information TSC possesses that indicates for-profit companies received TSDB information.***

**Supplemental Response:** As previously explained, TSC does not provide TSDB information to any for-profit entities. It is treated as law enforcement sensitive, and watchlist status is generally treated as Sensitive Security Information (SSI) pursuant to 49 U.S.C. §114(r) and 49 C.F.R. part 1520. Moreover, as stated in the Groh deposition, TSC contracts with Strategic Operation Solutions and with Sotera Defense to provide personnel to staff certain TSC positions. Some employees of those for-profit companies who are staffing TSC positions have access to TSDB information in their capacity as

TSC staff, but the companies themselves do not otherwise have access to TSDB information.

In addition, as stated in TSC's response to Interrogatory 2 in the Plaintiffs' First Set of Interrogatories to TSC, the TSC exports a subset of TSDB data to the National Crime Information Center (NCIC), a nationwide, computerized information system administered by the FBI. This export from TSC to the NCIC is referred to as the Known or Suspected Terrorist (KST) File.

Detailed information about the NCIC can be found at <https://www.fbi.gov/services/cjis/ncic>. It is TSC's understanding that in order for an entity to access information in the NCIC, the entity must obtain an Originating Agency Identifier (ORI) from the FBI's Criminal Justice Information Services (CJIS) Division. In order for a private entity to obtain an ORI that provides access to all NCIC Files, including the KST File, that entity must be providing services for the administration of criminal justice in accordance with 28 C.F.R. § 20.33, or the entity must be a qualified police department of a railroad or private college or university, pursuant to 28 U.S.C. § 534(e).

While an entity applying to the CJIS Division for an ORI is required to indicate whether it is a governmental or private entity, it is not required to indicate whether it is for-profit or not-for-profit. Thus, TSC's understanding is that the CJIS Division does not collect information as to which private companies with access to the NCIC KST File are "for-profit." However, the types of non-governmental entities with access to the NCIC KST File include: private correctional facilities; private security services for governmental facilities and hospitals; companies providing criminal justice dispatching

services or data processing/information services to governmental criminal justice agencies; private probation and pretrial services companies; private city attorneys; and other entities similarly performing criminal justice services.

Those entities which are authorized to access NCIC pursuant to 28 C.F.R. § 20.33(a)(7), may only access NCIC pursuant to an agreement with a governmental criminal justice agency (CJA) or a noncriminal justice governmental agency performing criminal justice dispatching services or data processing/information services for governmental criminal justice agencies. The private contractor is, thus, providing services on behalf of or in support of a CJA.

Pursuant to 28 C.F.R. § 20.33(a)(7), the agreement between the private contractor and the governmental agency must incorporate a security addendum approved by the Attorney General of the United States, which limits the use of the NCIC information, ensures the security and confidentiality of the information consistent with regulations and CJIS security policies, provides for sanctions, and contains such other provisions as the Attorney General may require. The power and authority of the Attorney General under this provision is exercised by the FBI Director (or the Director's designee). The CJIS Security Addendum, found at Appendix H to the CJIS Security Policy, see [https://www.fbi.gov/file-repository/cjis-security-policy\\_v5-7\\_20180816.pdf/view](https://www.fbi.gov/file-repository/cjis-security-policy_v5-7_20180816.pdf/view), is the uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General, which contains the provisions required under 28 C.F.R. § 20.33(a)(7).

Private contractors who perform criminal justice functions must meet the same training and certification criteria required by governmental agencies performing a similar

function, and are subject to the same audit review as are local user agencies. All private contractors who perform criminal justice functions are required to acknowledge, by signing the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum.

In addition, certain police departments of railroads and private colleges or universities can obtain access to the NCIC, including the KST File, pursuant to 28 U.S.C. § 534(a). Police departments that obtain NCIC access under that provision must comply with the CJIS Security Policy.

TSC's understanding is that there are currently 1441 ORIs issued to private entities pursuant to either 28 C.F.R. § 20.33 or 28 U.S.C. § 534. However, the number of private entities issued ORIs under these provisions is less than 1441 as in many cases multiple ORIs have been issued to the same entity.

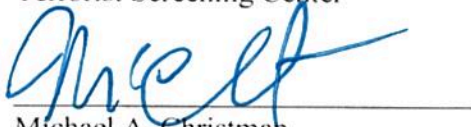
As stated in TSC's response to Interrogatory 2 in the Plaintiffs' First Set of Interrogatories to TSC, TSC exports TSDB data to the Department of Homeland Security (DHS). It is TSC's understanding that DHS may share certain information with "for profit" entities in certain limited circumstances, when necessary to facilitate its mission. For example, it is TSC's understanding that TSA provides a subset of TSDB information to regulated U.S. aircraft operators for the purpose of vetting airline employees who may have access to SSI, to regulated airport operators for the purpose of vetting non-traveling or other individuals who are authorized to have access to the airport, and to regulated U.S. aircraft operators operating charters and other flights under a TSA-authorized security program on aircraft that are not covered by Secure Flight for the purpose of vetting employees and traveling passengers against the No Fly and Selectee subsets of the TSDB. It is also TSC's understanding that TSA permits regulated entities who are

authorized to receive subsets of the TSDB to share this information with authorized representatives they have contracted to perform the vetting function on their behalf. All parties authorized to receive TSDB information by TSA must safeguard this information from unauthorized disclosure in accordance with the provisions of 49 CFR Part 1520. Other than as described above, TSC is not aware of any for-profit companies with access to TSDB information. Specifically, TSC is not aware of any mechanism, policy, or practice that would permit TSDB information to be shared with car dealerships or banks.

For the Responses:



Timothy P. Groh  
Deputy Director for Operations  
Terrorist Screening Center



Michael A. Christman  
Deputy Assistant Director, Operational Programs Branch  
Criminal Justice Information Services Division